Docket No.: 248588007US
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	Boscolo et al.		
Application No.:	09/800,754	Conf. No.:	3879
Filed:	March 6, 2001	Art Unit:	2134
For:	REMOTE MANAGEMENT OF PROPERTIES, SUCH AS PROPERTIES FOR ESTABLISHING A VIRTUAL PRIVATE NETWORK	Examiner:	D. Y. Jung

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This brief is in furtherance of the Notice of Appeal filed in this case on October 6, 2006. The fees required under § 41.20(b)(2) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

I. REAL PARTY IN INTEREST

The rights of the inventors in this application have been assigned to Watchguard Technologies, Inc., of Seattle, Washington, as originally recorded at reel 012214, frame 0383.

II. RELATED APPEALS AND INTERFERENCES

Neither Appellants, Appellants' legal representative, nor the above-identified Assignee are aware of other appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the present appeal.

III. STATUS OF CLAIMS

Claims 1-43 have been presented. Claims 14, 26, 27, 32 and 33 have been canceled during prosecution. Claims 1-13, 15-25, 28-31 and 34-43 are therefore presently pending, and stand twice rejected.

Claims 1-13, 15-25 and 34-43 are the subject of the present appeal. The text of these claims is set forth below in the Claims Appendix.

IV. STATUS OF AMENDMENTS

No amendments have been filed subsequent to an Office Action dated April 7, 2006.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Each independent claim being appealed is paraphrased below, with citations to the corresponding portions of the specification and drawing as required by 37 C.F.R. § 41.37(c)(1)(v). These citations are provided in order to illustrate specific examples and embodiments of the recited claim language, and are not intended to limit the claims.

A. Overview of the Invention

The rejected claims are directed to techniques for centrally managing properties of a Virtual Private Network (VPN) established between two or more private networks. Some of the techniques are directed to automatically updating the properties of nodes within the VPN called managed property clients. Each managed property client has an overall property set that it maintains and uses in aspects of its operation that includes properties that are remotely managed by a server. For example, the properties managed for the managed property clients by the server may specify how to establish, maintain, notify, or

terminate VPNs between selected clients. In some cases, a managed property client periodically requests property updates from a server, enclosing an indication of the generation date of its current overall property set. In response, the server may instruct the managed property client to transmit its current overall property set and, when the server receives the managed property client's current overall property set, the server makes a copy and substitutes for any updated property. If the resultant new overall property set differs from the current overall property set, the server sends the overall property set to the managed property client for use by the managed property client.

B. Independent Claims on Appeal

1. Claim 1

Claim 1 is directed to a method in a computing system for updating properties used by a subject computer system using a helper computer system. The method comprises maintaining a set of current properties on the subject computer system (*See e.g.*, Specification, 3:8-10), and, in the helper computer system, receiving new properties for the subject computer system. The method also comprises transmitting the current properties from the subject computer system to the helper computer system (*See e.g.*, *Id.*, 5:14-15, Fig. 3), and, in the helper computer system, merging the received new properties into a copy of the transmitted current properties, comparing the received current properties to the copy of the received current properties into which were merged the received new properties and, if the received current properties to the copy of the received current properties differ, transmitting the copy of the current properties into which were merged the received new properties to the subject computer system (*See e.g.*, *Id.*, 3:13-17, 5:16-18, Fig. 3). The method further comprises, in the subject computer system, adopting the transmitted copy of the current properties into which were merged the received new properties (*See e.g.*, *Id.*, 5:18-19, Fig. 3).

2. Claim 8

Claim 8 is directed to a method in a computing system for remotely managing properties for a subject computer system. The method comprises receiving a property update inquiry from the subject computer system, the inquiry indicating a time at which properties in use by the subject computer system were updated (*See e.g., Id.*, 4:28-5:6, Fig. 3). The method also comprises comparing the indicated time to an update time for managed properties, and, if the indicated time is earlier than the update time, retrieving a copy of the existing properties used by the subject computer system, merging managed properties into the copy of the existing properties, and sending the merged properties to the subject computer system (*See e.g., Id.*, 5:7-22, Fig. 3).

3. Claim 11

Claim 11 is directed to a method in a server computer system for establishing a virtual private network between a first private network having a first security device and a second private network having a second security device. The method comprises generating properties for the first security device to direct the participation of the first security device in the virtual private network, and generating properties for the second security device to direct the participation of the second security device in the virtual private network. The method also comprises distributing the properties generated for the first security device to the first security device for use by the first security device to participate in the virtual private network. The method further comprises distributing the properties generated for the second security device to the second security device for use by the second security device to participate in the virtual private network, wherein the distributing includes transmitting the generated properties to the security devices in response to inquiries from the security devices at times subsequent to the generating. (*See e.g., Id.*, 5:23-29:17, Fig. 4.)

4. Claim 25

Claim 25 is directed to a computer-readable medium whose contents cause a server computer system to establish a virtual private network between a first private network having a first security device and a second private network having a second security device. The contents cause the server computer system to generate properties for the first security device to direct the participation of the first security device in the virtual private network, and generate properties for the second security device to direct the participation of the second security device in the virtual private network. The contents cause the server computer system to also distribute the properties generated for the first security device to the first security device for use by the first security device to participate in the virtual private network. The contents cause the server computer system to further distribute the properties generated for the second security device to the second security device for use by the second security device to participate in the virtual private network, wherein the distributing includes transmitting the generated properties to the security devices in response to inquiries from the security devices at times subsequent to the generating. (*See e.g.*, *Id.*, 5:23-29:17, Fig. 4.)

5. Claim 34

Claim 34 is directed to a method in a distinguished computing system for managing properties used by the distinguished computer system in its operation. The method comprises maintaining a first set of properties, receiving from a separate computing system a second set of properties, and using both the first set of properties and the second set of properties in the operation of the distinguished computing system. (*See e.g.*, *Id.*, 4:28-5:22, Fig. 3.)

6. Claim 39

Claim 39 is directed to a method in a manager computing system for participating in the management of properties used by a client computing system. The method comprises determining that properties of the client computing system managed by the manager

computing system should be updated, and instructing the client computing system to use in its operation manager-managed properties updated in accordance with the determination, in conjunction with properties of the client computing system managed by the client computing system. (*See e.g.*, *Id.*, 4:28-5:22, Fig. 3.)

7. Claim 42

Claim 42 is directed to a system for managing properties for a distinguished computing system. The system comprises the distinguished computing system and a managing computing system. The distinguished computing system utilizes both locally-managed properties and remotely-managed properties, and manages the locally-managed properties. The manager computing system is communicatively connected to the distinguished computing system, and manages the remotely-managed properties. (*See e.g.*, Specification, 4:28-5:22, Fig. 3.)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. The Examiner's Rejections

The Examiner has rejected claims 1-13, 15-25 and 34-43 under 35 U.S.C. § 102(b) over U.S. Patent No. 6,701,358 to Poisson et al. ("Poisson").

B. The issue on Appeal

1. Is the rejection of claims 1-13, 15-25 and 34-43 under 35 U.S.C. § 102(b) over Poisson proper?

VII. ARGUMENT

A. Rejections Under 35 U.S.C. § 102(b)

1. Legal Standards for Anticipation

35 U.S.C. § 102(b) provides:

A person shall be entitled to a patent unless—

. . .

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States,

Anticipation requires that each claim element must be identical to a corresponding element in the applied reference. *Glaverbel Société Anonyme v. Northlake Mktg. & Supply, Inc.*, 45 F.3d 1550, 1554 (Fed. Cir. 1995). Indeed, the failure to mention "a claimed element (in) a prior art reference is enough to negate anticipation by that reference." *Atlas Powder Co. v. E.I. duPont De Nemours*, 750 F.2d 1569, 1574 (1984). To establish a *prima facie* case of anticipation, the Examiner must identify where "each and every facet of the claimed invention is disclosed in the applied reference." *Ex parte Levy,* 17 U.S.P.Q.2d 1461, 1462 (Bd. Pat. App. & Interf. 1990).

Under these standards, Appellants' invention would not have been anticipated. The Examiner has not identified a prior art reference that identically discloses all the elements of claims 1-13, 15-25 and 34-43. Therefore, these claims should be allowed.

B. Overview of the Cited Reference

1. The Poisson Reference

Poisson describes a method for managing a VPN by transmitting configuration information for at least one VPN function to multiple computers providing the VPN function. (Poisson, Abstract, 1:47-51.) In Poisson, an extranet switch manager centralizes the management of different extranet switches and is used to bulk configure multiple extranet switches, prepare reports describing the extranet switches, provide convenient access to individual switch configuration mechanisms, and provide an intuitive representation of VPN elements. (*Id.*, 2:58-61.)

Although Poisson describes configuring extranet switches, Poisson's configuration method is significantly different than Appellants' claimed management techniques. Poisson merely indicates that the extranet switch manager allows an administrator to input

configuration information. (*Id.*, 2:58-66.) According to Poisson, the extranet switch manager transmits the input configuration information to the appropriate extranet switches. (*Id.*, 4:49-53.) Poisson does not contain any teaching or suggestion of the extranet switch manager merging the input configuration information for a subject extranet switch with a copy of the existing configuration information of the subject extranet switch received from the subject extranet switch, transmitting the generated configuration information to the subject extranet switch in response to an inquiry from the subject extranet switch at times subsequent to generating the configuration information, or using both configuration information maintained by the subject extranet switch and configuration information received from a separate computing system in the operation of the subject extranet switch. Indeed, having Poisson's extranet switch manager merge the input configuration information with a copy of the existing configuration information received from the subject extranet switch, transmit the generated configuration information to the subject extranet switch in response to an inquiry from the subject extranet switch at times subsequent to generating the configuration information, or use both configuration information maintained by the subject extranet switch and configuration information received from a separate computing system in the operation of the subject extranet switch would be counter to Poisson's stated advantages of its bulk configuration (1) enabling an administrator to configure a large number of extranet switches by specifying a single common configuration, (2) reducing the amount of time needed to configure the extranet switches, and (3) reducing the errors that might occur through repeated individual configuration. (*Id.*, 2:17-23, 3:38-44.)

C. Rejection of the Claims

1. Claims 1-7

a. The Examiner has Failed to Identify Elements of Poisson that are Identical to the Elements Recited by Claims 1-7, and Thereby Failed to Establish a *Prima Facie* Case of Anticipation with Respect to Poisson

In the Office Action dated April 7, 2006, the Examiner rejected claims 1-7 under 35 U.S.C. § 102(b) over Poisson. In this Office Action, the Examiner responded to Appellants' argument that Poisson does not teach merging the new properties into a copy of the existing properties received from a subject computer system, with the following statement:

> Applicant asserts that Poisson does not, rather than "cannot", teach determining whether the new properties differ from the properties already in use. This argument, of course, goes to the issue of obviousness. The Office respectfully requests Applicant to explain why this feature (of determining whether the new properties differ from the properties already in use) would not be inherent. Poisson is clearly directed to a portion of a complete system. Poisson does not forbid a functioning system. In a functioning system, this feature (of determining whether the new properties differ from the properties already in use) is necessary. Necessary features are inherent.
>
> Perhaps Applicant does not agree that this feature is necessary. The Office's view is shaped from the fact that keeping track of properties is necessary and that such keeping track of new properties would require this feature (of determining whether the new properties differ from the properties already in use). The Office awaits Applicant's explanation (or amendment or any other appropriate action) regarding this issue.

(Office Action, April 7, 2006, p. 2.)

These statements do not satisfy the Examiner's burden of establishing a *prima facie* case of anticipation. The Federal Circuit has stated that, "[i]nherency may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient to establish inherency." *See Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1269, 20 U.S.P.Q.2d 1746, 1749 (Fed. Cir. 1991). Rather, inherency requires that "the missing descriptive matter is necessarily

present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." *Id.* at 1268, 1749.

In contrast to the Examiner's position, the feature of determining whether the new properties differ from the properties already in use is not necessary to any feature expressly disclosed by Poisson and, therefore, not inherent. Appellants are aware of numerous other ways of updating the properties used by a subject computer system without determining whether the new properties differ from the properties already in use by the subject computer system. As one example, Poisson, which the Examiner relies upon in the 35 U.S.C. § 102(b) rejection of claims 1-7, teaches another method of updating the properties used by a subject computer system without determining whether the new properties differ from the properties already in use by the subject computer system. As discussed above in Section VII.B.1, Poisson teaches an extranet switch manager that transmits configuration information, as input by and received from an administrator, to the appropriate extranet switches. In Poisson, the extranet switch manager does not process the input configuration information to determine whether the input configuration information differs from the configuration information already in use by the appropriate extranet switches. Indeed, as discussed above in Section VII.B.1, determining whether the input configuration information differs from the configuration information already in use by the appropriate extranet switches would be counter to the purported advantages sought after and provided by Poisson.

Other than the Examiner's response to Appellants' argument stated above, the entirety of the Examiner's claim rejections is as follows:

> Claims 1-13, 15-25, 28-31, 34-43 are rejected because of the features of the prior art as noted in the previous section. The claims are rejected under 35 USC 102.

(Office Action, April 7, 2006, p. 3.) Notwithstanding these statements, the Examiner has failed to provide any indication of how Poisson teaches merging the new properties into a copy of the existing properties received from a subject computer system.

As such, the Examiner has not presented a *prima facie* case of anticipation, and the rejection of claims 1-7 should be reversed.

b. Poisson Fails to Disclose All of the Elements Recited by Claims 1-7 and Is Therefore Incapable of Supporting any Proper Rejection Under 35 U.S.C. § 102(b)

Poisson fails to disclose all of the elements recited by claims 1-7. Claims 1-7 recite a helper computer system merging the received new properties into a copy of the transmitted current properties. As discussed above in Section VII.B.1, Poisson does not contain any disclosure of the extranet switch manager receiving the existing configuration information of a subject extranet switch from the extranet switch, and merging the input configuration information for the subject extranet switch with a copy of the received existing configuration information of the subject extranet switch. In a similar manner, Poisson does not teach the helper computer system merging the received new properties into a copy of the current properties received from the subject computer system. For at least this reason, Poisson fails to support any proper rejection of claims 1-7 under 35 U.S.C. § 102(b).

2. Claims 8-10

a. The Examiner has Failed to Identify Elements of Poisson that are Identical to the Elements Recited by Claims 8-10, and Thereby Failed to Establish a *Prima Facie* Case of Anticipation with Respect to Poisson

The rejection of claims 8-10 is improper because the Examiner has failed to establish a *prima facie* case for anticipation. Similar to the discussion above with respect to claims 1-7, the Examiner has not cited any portion of Poisson that teaches retrieving a copy of the existing properties used by the subject computer system and merging managed properties into the copy of the existing properties, as recited in the claims. As

such, the Examiner has not presented a *prima facie* case of anticipation, and the rejection of claims 8-10 should be reversed.

b. Poisson Fails to Disclose All of the Elements Recited by Claims 8-10 and Is Therefore Incapable of Supporting any Proper Rejection Under 35 U.S.C. § 102(b)

As discussed above, Poisson does not contain any disclosure of the extranet switch manager receiving the existing configuration information of a subject extranet switch from the extranet switch and merging the input configuration information for the subject extranet switch with a copy of the received existing configuration information of the subject extranet switch. In a similar manner, Poisson does not teach retrieving a copy of the existing properties used by the subject computer system and merging managed properties into the copy of the existing properties. For at least this reason, Poisson fails to support any proper rejection of claims 8-10 under 35 U.S.C. § 102(b).

3. Claims 11-13 and 15-25

a. The Examiner has Failed to Identify Elements of Poisson that are Identical to the Elements Recited by Claims 11-13 and 15-25, and Thereby Failed to Establish a *Prima Facie* Case of Anticipation with Respect to Poisson

In the Office Action dated April 7, 2006, the Examiner rejected claims 11-13 and 15-25 under 35 U.S.C. § 102(b) over Poisson. In this Office Action, the only explanation of the rejection is the following statement:

> Claims 1-13, 15-25, 28-31, 34-43 are rejected because of the features of the prior art as noted in the previous section. The claims are rejected under 35 USC 102.

(Office Action, April 7, 2006, p. 3.) With respect to claims 11-13 and 15-25, this statement does not satisfy the Examiner's burden of establishing a *prima facie* case of anticipation. Appellants amended these claims to recite "wherein the distributing includes transmitting the generated properties to the security devices in response to inquiries from the security devices at times subsequent to the generating" in its response to a non-final Office Action

dated December 20, 2004. (Amendment, April 21, 2005.) The Examiner's only explanation of the rejection of these claims subsequent to the amendment to the claims was the following statement: "the amended claims that were previously rejected under 35 USC 102 (before amendment) are now rejected under 35 USC 103." (Office Action, July 26, 2005, p. 2.) Because Appellants introduced the amendments subsequent to the December 20, 2004 Office Action, the amended feature could not have been, and was not addressed by the Examiner in the Examiner's 35 U.S.C. § 102(b) rejection in the December 20, 2004 Office Action. By summarily stating that the claims are now rejected under 35 USC 103 in the July 26, 2005 Office Action, and then rejected under 35 USC 102 in the April 7, 2006 Office Action, the Examiner has failed to provide any indication of how Poisson teaches the claimed "transmitting the generated properties to the security devices in response to inquiries from the security devices at times subsequent to the generating."

As such, the Examiner has not presented a *prima facie* case of anticipation, and the rejection of claims 11-13 and 15-25 should be reversed.

b. Poisson Fails to Disclose All of the Elements Recited by Claims 11-13 and 15-25 and Is Therefore Incapable of Supporting any Proper Rejection Under 35 U.S.C. § 102(b)

Poisson fails to disclose all of the elements recited by claims 11-13 and 15-25. Claims 11-13 and 15-25 recite a server computer system transmitting the generated properties to the security devices in response to inquiries from the security devices at times subsequent to the generating. As discussed above in Section VII.B.1, Poisson does not contain any disclosure of the extranet switch manager transmitting the generated configuration information to the subject extranet switch in response to an inquiry from the subject extranet switch at times subsequent to generating the configuration information. In a similar manner, Poisson does not teach a server computer system transmitting the generated properties to the security devices in response to inquiries from the security devices at times subsequent to the generating. For at least this reason, Poisson fails to support any proper rejection of claims 11-13 and 15-25 under 35 U.S.C. § 102(b).

4. Claims 34-43

a. The Examiner has Failed to Identify Elements of Poisson that are Identical to the Elements Recited by Claims 34-43, and Thereby Failed to Establish a *Prima Facie* Case of Anticipation with Respect to Poisson

In the Office Action dated April 7, 2006, the Examiner rejected claims 34-43 under 35 U.S.C. § 102(b) over Poisson. In this Office Action, the only explanation of the rejection is the following statement:

> Claims 1-13, 15-25, 28-31, 34-43 are rejected because of the features of the prior art as noted in the previous section. The claims are rejected under 35 USC 102.

(Office Action, April 7, 2006, p. 3.) With respect to claims 34-43, this statement does not satisfy the Examiner's burden of establishing a *prima facie* case of anticipation. These claims recite the use of both properties maintained by the distinguished computing system and properties received from a separate computing system in the operation of the distinguished computing system. For example, claims 34-38 recite "using both the first set of properties and the second set of properties in the operation of the distinguished computing system," claims 39-41 recite "instructing the client computing system to use in its operation manager-managed properties updated in accordance with the determination, in conjunction with properties of the client computing system managed by the client computing system," and claims 42 and 43 recite "the distinguished computing system, which utilizes both locally-managed properties and remotely-managed properties, and which manages the locally-managed properties." The Examiner has failed to provide any indication of how Poisson teaches the use of both properties maintained by the distinguished computing system and properties received from a separate computing system in the operation of the distinguished computing system.

The only other possible explanation for the rejection of these claims is the following statement:

> As to claim(s) 42:
>
> Locally managed properties and remotely-managed properties / The bulk configuration information can be specified by a user, provided by a program that automatically configures switches, or copied from configuration information of a previously configured switch (Col 6, Line 19-23, '358)
>
> Manager computer system communicatively connected to the distinguished computer system which manages the remotely-managed properties / VPN manager (Fig 1, Element 116, '358)

(Office Action, December 22, 2004, pp. 5-6.) These statements also do not satisfy the Examiner's burden of establishing a *prima facie* case of anticipation with regard to these claims. The sections of Poisson referenced by the Examiner do not teach the use of both properties maintained by the distinguished computing system and properties received from a separate computing system in the operation of the distinguished computing system. First, Poisson, at col. 6, lines 19-23, indicates that the switches may use LDAP authentication by storing remote access profiles in an external LDAP server and querying the LDAP server for the access profile information when a user attempts to establish a tunnel connection. Contrary to the Examiner's assertion, Poisson's discussion of storing and accessing profile information to perform LDAP authentication does not teach the use of both properties maintained by the distinguished computing system and properties received from a separate computing system in the operation of the distinguished computing system. Second, although the extranet switch manager (Poisson, Fig. 1, Element 116) allows for the remote management of extranet switches, Poisson contains no indication that the extranet switch manager uses both configuration information maintained by the extranet switch and its remotely-managed configuration information in the management of the extranet switch. As a result, Poisson does not teach an extranet switch using both configuration information maintained by the extranet switch and remotely-managed configuration information received from the extranet switch manager in the operation of the extranet switch.

As such, the Examiner has not presented a *prima facie* case of anticipation, and the rejection of claims 34-43 should be reversed.

b. Poisson Fails to Disclose All of the Elements Recited by Claims 34-43 and Is Therefore Incapable of Supporting any Proper Rejection Under 35 U.S.C. § 102(b)

Poisson fails to disclose all of the elements recited by claims 34-43. Claims 34-43 recite the use of both properties maintained by the distinguished computing system and properties received from a separate computing system in the operation of the distinguished computing system. As discussed above in Section VII.B.1, Poisson does not contain any disclosure of an extranet switch using both configuration information maintained by the extranet switch and remotely-managed configuration information received from the extranet switch manager in the operation of the extranet switch. In a similar manner, Poisson does not teach a distinguished computing system using both properties maintained by the distinguished computing system and properties received from a separate computing system in the operation of the distinguished computing system. For at least this reason, Poisson fails to support any proper rejection of claims 34-43 under 35 U.S.C. § 102(b).

VIII. SUMMARY

Each of claims 1-13, 15-25 and 34-43 has been improperly rejected, both (a) in that the Examiner has failed to provide prior art references that disclose all of the elements of these claims, and (b) in that the cited references would not support any rejection of these claims. Accordingly, Appellants seek the reversal of the rejection of claims 1-13, 15-25 and 34-43.

Dated: December 13, 2006

Respectfully submitted,

By _____
Do Te Kim
Registration No.: 46,231
PERKINS COIE LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-8000
(206) 359-7198 (Fax)
Attorneys for Appellants

CLAIMS APPENDIX

Claims Involved in the Appeal of Application Serial No. 09/800,754

1. (Original) A method in a computing system for updating properties used by a subject computer system using a helper computer system, comprising:

maintaining a set of current properties on the subject computer system;

in the helper computer system, receiving new properties for the subject computer system;

transmitting the current properties from the subject computer system to the helper computer system;

in the helper computer system,

merging the received new properties into a copy of the transmitted current properties;

comparing the received current properties to the copy of the received current properties into which were merged the received new properties;

if the received current properties to the copy of the received current properties differ, transmitting the copy of the current properties into which were merged the received new properties to the subject computer system; and

in the subject computer system, adopting the transmitted copy of the current properties into which were merged the received new properties.

2. (Original) The method of claim 1 wherein the comparing includes:

generating a digest of each the received current properties to the copy of the received current properties into which were merged the received new properties; and

comparing the generated digests.

3. (Original) The method of claim 2 wherein the digests are generated using a hashing function.

4. (Original) The method of claim 2 wherein the digests are generated using an MD5 hashing function.

5. (Original) The method of claim 2 wherein the merging includes:

deleting from the copy of the current properties any properties managed by the helper computer system; and

adding properties including the new properties to the copy of the current properties.

6. (Original) The method of claim 5 wherein the deleting includes deleting properties in the copy of the current properties identified by administrative properties among the current properties.

7. (Original) The method of claim 1 wherein the merging includes adding to the copy of the current properties administrative properties identifying other properties added to the copy of the current properties.

8. (Original) A method in a computing system for remotely managing properties for a subject computer system, comprising:

receiving a property update inquiry from the subject computer system, the inquiry indicating a time at which properties in use by the subject computer system were updated;

comparing the indicated time to an update time for managed properties;

if the indicated time is earlier than the update time,

retrieving a copy of the existing properties used by the subject computer system;

merging managed properties into the copy of the existing properties; and

sending the merged properties to the subject computer system.

9. (Original) The method of claim 8 wherein the merged properties sent to the subject computer system include an instruction to adopt the merged properties.

10. (Original) The method of claim 8, further comprising comparing the merged properties to the existing properties, and wherein the sending is only performed if the merged properties and the existing properties are not the same.

11. (Previously Presented) A method in a server computer system for establishing a virtual private network between a first private network having a first security device and a second private network having a second security device, comprising:

generating properties for the first security device to direct the participation of the first security device in the virtual private network;

generating properties for the second security device to direct the participation of the second security device in the virtual private network;

distributing the properties generated for the first security device to the first security device for use by the first security device to participate in the virtual private network; and

distributing the properties generated for the second security device to the second security device for use by the second security device to participate in the virtual private network,

wherein the distributing includes transmitting the generated properties to the security devices in response to inquiries from the security devices at times subsequent to the generating.

12. (Original) The method of claim 11 wherein the properties generated for the first security device are distinct from the properties generated for the second security device.

13. (Original) The method of claim 11 wherein the generated properties are adopted by both security devices to establish the virtual private network.

14. (Canceled)

15. (Original) The method of claim 11 wherein the distributing includes transmitting the generated properties to the security devices in response to the generation of the properties.

16. (Original) The method of claim 11, further comprising receiving a single set of VPN specifications in the server computer system,

and wherein the method is performed without regard for any user input received subsequent to receiving the single set of VPN specifications.

17. (Original) The method of claim 11 wherein the generation of properties for each security device includes:

selecting a property template; and

populating the selected property template with information specific to the first private network and/or information specific to the second private network.

18. (Original) The method of claim 11 wherein the generated properties include security properties relating to the protection of data traveling in the virtual private network.

19. (Original) The method of claim 18 wherein the security properties specify encryption parameters for data traveling in the virtual private network.

20. (Original) The method of claim 11 wherein the generated properties include resource properties relating to sources and destinations in the private networks for data traveling in the virtual private network.

21. (Original) The method of claim 20 wherein the resource properties specify addresses of network nodes within the private networks that may send and receive data traveling in the virtual private network.

22. (Original) The method of claim 11 wherein the generated properties include service properties relating to classes of data that may travel in the virtual private network.

23. (Original) The method of claim 22 wherein the service properties specify network protocols for which data may travel in the virtual private network.

24. (Original) The method of claim 11, further comprising performing the generating and distributing for one or more additional security devices in order to establish the virtual private network between more than two private networks.

25. (Previously Presented) A computer-readable medium whose contents cause a server computer system to establish a virtual private network between a first private network having a first security device and a second private network having a second security device by:

generating properties for the first security device to direct the participation of the first security device in the virtual private network;

generating properties for the second security device to direct the participation of the second security device in the virtual private network;

distributing the properties generated for the first security device to the first security device for use by the first security device to participate in the virtual private network; and

distributing the properties generated for the second security device to the second security device for use by the second security device to participate in the virtual private network,

wherein the distributing includes transmitting the generated properties to the security devices in response to inquiries from the security devices at times subsequent to the generating.

26. – 27. (Canceled)

28. (Previously Presented) A method in a single manager computing system for managing properties for a plurality of managed computer systems, comprising, reiteratively:

receiving new managed properties for an identified managed computer system;

determining whether the new managed properties received differ from those in use by the identified managed computer system; and

delivering the received new managed properties to the identified managed computer system,

wherein the new managed properties are delivered only if it is not determined that the new managed properties received differ from those in use by the identified managed computer system.

29. (Original) The method of claim 28 wherein at least one of the managed computer systems is a dedicated network security device.

30. (Original) The method of claim 28 wherein, for each managed computer system, the managed properties are a proper subset of a set properties used by the managed computer system, and wherein the delivering includes:

receiving the set of properties used by the managed computer system;

substituting for managed properties in the set of properties used by the managed computer system new managed properties received by the manager computer system; and

conveying to the managed computer system the set of properties used by the managed computer system in which the new managed properties have been substituted.

31. (Original) The method of claim 28, further comprising cacheing the received new managed properties until delivery.

32 – 33. (Canceled)

34. (Original) A method in a distinguished computing system for managing properties used by the distinguished computer system in its operation, comprising:

maintaining a first set of properties;

receiving from a separate computing system a second set of properties; and

using both the first set of properties and the second set of properties in the operation of the distinguished computing system.

35. (Original) The method of claim 34, further comprising:

updating one or more properties among the first set of properties at the initiation of the distinguished computing system; and

using the updated properties in the operation of the distinguished computing system.

36. (Original) The method of claim 34, further comprising:

receiving one or more updated properties from the separate computing system; and

using the updated properties in the operation of the distinguished computing system.

37. (Original) The method of claim 36 wherein the updated properties specify the establishment of a virtual private network between the distinguished computing system and an additional computing system.

38. (Original) The method of claim 34, further comprising:

sending the first and second sets of properties as a configuration to the separate computing system;

receiving from the separate computer system a replacement configuration, in which properties of the second set have been modified; and

using the properties in the replacement configuration in the operation of the distinguished computing system.

39. (Original) A method in a manager computing system for participating in the management of properties used by a client computing system, comprising:

determining that properties of the client computing system managed by the manager computing system should be updated; and

instructing the client computing system to use in its operation manager-managed properties updated in accordance with the determination, in conjunction with properties of the client computing system managed by the client computing system.

40. (Original) The method of claim 39, further comprising:

receiving from the client computing system a client configuration comprising the manager-managed properties and client-managed properties in use by the client computing system;

incorporating in the received client configuration the manager-managed properties updated in accordance with the determination to produce an updated client configuration; and

returning the updated client configuration to the client computing system with an instruction to use the updated client configuration in the operation of the client computing system.

41. (Original) The method of claim 39 wherein the updated properties specify the establishment of a virtual private network between the client computing system and an additional computing system.

42. (Original) A system for managing properties for a distinguished computing system, comprising:

the distinguished computing system, which utilizes both locally-managed properties and remotely-managed properties, and which manages the locally-managed properties; and

a manager computing system communicatively connected to the distinguished computing system, which manages the remotely-managed properties.

43. (Original) The method of claim 42 wherein the distinguished computing system is a specialized network security device.

EVIDENCE APPENDIX

No evidence has been entered or is being relied upon in the present appeal.

RELATED PROCEEDINGS APPENDIX

There are no decisions rendered by a court or the Board in any proceeding identified in the Related Appeals and Interferences section.